Naval War College Review

Volume 53
Number 3 *Summer*

Article 3

2000

Whom the Gods Would Destroy

Robert D. Critchlow

Whom the Gods Would Destroy

An Information Warfare Alternative for Deterrence and Compellence

Major Robert D. Critchlow, U.S. Air Force

SINCE THE END OF THE COLD WAR, the threat from weapons of mass destruction (WMD) has expanded beyond the massive arsenal of the former Soviet Union to many nations who are possessors—declared and undeclared—of nuclear, biological, or chemical weapons and the means to deliver them, or are attempting to acquire them. The United States therefore requires the ability to deter these smaller WMD-owning adversaries and, when necessary, to compel them to comply with its will or that of the international community. However, as has been widely noted, the utility and credibility of the U.S. nuclear arsenal for these ends are growing smaller, due to the success of arms control and public abhorrence of the nuclear instrument. Therefore, an alternative strategy is required, one that provides a responsive intermediate step on the escalation ladder.

Information warfare (IW) can provide that alternative. Like nuclear weapons, information warfare techniques can, at least theoretically, punish an adversary by striking speedily at his "centers of gravity"—leadership, command and control, national infrastructure, or industry—without defeating conventional forces in the field. It provides an alternative that the public is likely to be more willing to accept than a nuclear response to WMD use by a small power. It also provides a proportionate response to hostile attacks against the U.S. information infrastructure.

The military community uses a variety of terms to describe relationships between warfare, information, and information technology.[1] Among them are "knowledge-based warfare" and "network-centric warfare," which imply the networking and exploitation of friendly communications, computers, intelligence, reconnaissance, and surveillance systems to maximize the effectiveness of traditional military arms.[2] The Department of Defense uses the terms "command and control warfare" and "information operations" in reference to the employment of psychological operations, electronic warfare, operations security, military deception, and physical destruction to strike command and control systems and affect the perceptions of hostile nations.[3] In this article, "information warfare" means specifically the use of computer network attacks and electronic warfare techniques against the military systems and, especially, the national information infrastructure of an antagonist.

The Proliferation Environment

The strategic environment that the United States faces at the turn of the millennium resembles that of the years of President Dwight D. Eisenhower's "New Look," before the Soviet Union exploded its first hydrogen bomb and developed an intercontinental missile. The nation is once more enjoying economic expansion; it is again in a position of military dominance, though this time through its conventional capability rather than its nuclear might. As in that period, there are few direct threats to the U.S. homeland. The United States of the 1950s faced international challenges in Korea and Indochina; the threats today are once more on the periphery.

As in the 1950s, when opponents on the periphery employed unconventional warfare to "end run" U.S. nuclear superiority, this nation's nuclear and conventional military capabilities are confronted

Major Critchlow is assigned to U.S. Strategic Command at Offutt Air Force Base, Omaha, Nebraska, as a space operations officer currently serving as a SIOP advisor in the USSTRATCOM Command Center. He is a former assistant professor at the U.S. Air Force Academy. A graduate of the College of Naval Command and Staff at the Naval War College, he holds a B.S. in physics from Carnegie Mellon University and an M.A. in history from Ohio State University. He wrote the original version of this article while a student at the Naval War College. He wishes to recognize the support and assistance of Dr. James Miskel, Dr. Roger Barnett, Staff Sgt. Robin Spangler, and his wife Janice in the preparation of this article.

This paper reflects the author's personal views and is not endorsed by U.S. Strategic Command or the Department of Defense.

today by an "asymmetrical" threat. Today, the proliferation of weapons of mass destruction increases the dangers and difficulties of the international arena. The number of nations that possess or are aggressively attempting to develop these weapons and ballistic missile systems to deliver them is expanding. James Woolsey, former Director of Central Intelligence, estimated in 1995 that twenty nations had or were developing WMD and delivery means. Fifteen nations already had ballistic missiles, and sixty-six possessed cruise missiles.[4]

> *Whom the gods would destroy they first make mad.*
>
> —*Euripides*

Since that time, India and Pakistan have openly demonstrated nuclear weapons capabilities. North Korea is estimated to have plutonium sufficient to build one or two nuclear weapons.[5] The U.S. homeland is expected to face additional ICBM threats from North Korea, Iran, and Iraq in the next fifteen years.[6] Of even higher probability is the launch of short and medium-range ballistic or cruise missiles at U.S. or allied military and civilian targets. Nonmissile delivery means is the most likely of all, as it is the easiest to achieve and avoids direct association with the perpetrator or sponsor.[7]

These technologies are spreading to smaller, radical, rogue states. Dr. Barry Schneider, in a coinage worthy of Ian Fleming, has christened these states "NASTIs": nuclear/biological/chemical-arming sponsors of terrorism and intervention. Iraq, Iran, and North Korea rank as charter members of this dubious club, while Libya, Cuba, and Syria are striving to become NASTI members.[8]

Iran uses its formal adherence to the Non-Proliferation Treaty as a camouflage under which to gain access to key technologies for its nuclear weapons program. Iran is actively improving its civilian nuclear energy program and cooperating with Russian and Chinese agencies to develop facilities that will both complete the nuclear fuel cycle and support weapon materials production.[9] It is expanding its chemical weapons program, though it signed the Chemical Weapons Convention; it has hundreds of tons of choking and blister agents in stock, and it is in the process of "weaponizing" its biological warfare research. In an example of the closeness of the NASTI fraternity, Iran has been able to buy Scud-C and No Dong-1 ballistic missiles from North Korea.[10]

As for Iraq, during the Gulf War it prepared Scud warheads containing chemical and biological agents for launching against Israel and Saudi Arabia, and it embarked on a crash effort to produce one or two nuclear warheads. Although its program was damaged in the war, Iraq preserved critical elements, as well as the expertise to re-create the rest. The CIA considers it likely that Iraq resumed its WMD programs after the air and cruise-missile strikes of Operation DESERT FOX in December 1998.[11] In fact, it has already acquired missile components in violation of UN sanctions. Of particular concern are recent revelations about the extent of the Iraqi anthrax program.[12]

Libya's budding WMD program also bears watching. The Libyans have a strong chemical weapons program, which is creating mustard gas and nerve gas. Their biological warfare and nuclear weapons are still in the research and development phase, but they are actively recruiting Russian scientists to speed their efforts. North Korea has provided Libya's program a boost by selling Scud and No Dong missiles. Particularly disturbing has been Libya's willingness to use these weapons, firing missiles at the island of Lampedusa and employing chemical weapons against Chad.[13]

The NASTIs will pose a narrowly focused nuclear threat, characterized by small, fission-type arsenals. These weapons will be able to hit troop concentrations, contaminating large areas with fallout, or to strike urban areas, causing mass casualties and terror. However, such weapons will be unable to threaten the American homeland for the foreseeable future: the missiles lack intercontinental range, and their nuclear weapons are too valuable to entrust to individuals to smuggle them in. Thus, the most likely uses for these weapons would be regional attacks to shape crises.[14]

The spread of missile technology multiplies the severity of the WMD threat to the interests, at least, of the United States. Missiles have a high probability of penetration, given the thinness of ballistic missile defenses. They can be fired at any time and in all weather. They can attack strategic targets in an adversary's rear areas, even if launched from the attacker's sovereign territory, where they are difficult to counterattack. Because of their short flight and warning times, they are particularly effective as terror weapons against civilian populations.[15]

WMD arsenals could create significant roadblocks to U.S. efforts to protect friends and safeguard regional interests. First, as Dean Wilkening and Kenneth Watman suggest, an adversary could employ these weapons to impede U.S. intervention in a crisis by interfering with deployments or attacking rear assembly areas. Second, as Robert Joseph argues, a rogue state could inflict casualties on U.S. servicemen or civilians of host nations in an attempt to sway American public opinion. Third, as Barry Schneider observes, the WMD-proliferating nation could use its arsenal for regional influence. Many nations have only one or two urban concentrations, making them effectively "one-bomb targets." A state with even a small arsenal can threaten such countries with national extinction; it might do so to intimidate U.S. allies, to fracture coalition building, or to compel neighbors to follow its lead. Last, as Schneider further notes, a regime confronted with defeat could use weapons of mass destruction as bargaining levers to preserve itself in a postwar settlement. In general, WMD arsenals allow outlaw nations to pursue asymmetric strategies against the United States.[16]

U.S. Objectives and Constraints in a Proliferation World

If the United States is to cope with this environment of WMD proliferation, it must be clear about its objectives. The primary goal is to remain able to pursue vital international interests in a world pervaded by weapons of mass destruction. This requires deterring rogue states from using such weapons against U.S. interests or partners. This deterrence, if successful, should reduce the value of acquiring WMD, by making them unusable for obtaining political goals.

As the United States continues nuclear arms reductions with the Russian Federation and refuses to modernize its arsenal, its overall capability in that area will decline. In any case, threats to use nuclear weapons could backfire, spurring opponents to acquire their own or to ally themselves with nuclear powers. The United States confronts international norms of nonuse that it helped to create and wants to preserve. Some would interpret an actual nuclear attack as a violation of the Non-Proliferation Treaty, which has joined the body of international law. An energetic nuclear deterrent posture, let alone an actual use of nuclear weapons, undoubtedly would lead to a domestic backlash, as well as international condemnation. To gauge the probable domestic response, consider the reactions during the Persian Gulf War to the Al Firdos bunker bombing or the "highway of death"—and multiply it. The American public abhors both nuclear weapons and high casualties, even among enemies.[17]

Beyond the policy constraints, practical constraints limit the utility of nuclear weapons for regional deterrence. MAD (mutual assured destruction) does not apply. As Philip Ritcheson argues, it is not mutual, because no regional power could hurt the United States as much as the United States could hurt it. Also, it is not assured: a U.S. threat to strike in retaliation would not be credible, because it would cause damage disproportionate to anything that could have been inflicted on the United States.[18]

Situational constraints also work against a U.S. regional nuclear deterrent. These constraints stem from differences between how the United States and a regional nuclear opponent view the risks. U.S. interests in regional contexts are typically peripheral; the regional player may be defending what it considers vital, bedrock values, in or near its homeland.[19]

A Strategy for Deterring the NASTIs

Given the environment and constraints of a proliferated world, the United States needs a new deterrence vehicle. The ideal instrument would be able to inflict more rapid and severe punishment than can conventional weapons but without the opprobrium that adheres to nuclear weapons. Facing an increased importance of nonstate actors and transnational organizations in the international system, such an instrument would have to be able to strike against such actors, again without the undesirable collateral effects of nuclear weapons.

It will be necessary, in addition, to modify the declaratory and practical elements of strategy to reflect both the wider range of threats to be deterred and the broader range of options for response. Current declaratory strategy is weak and vague. During the Gulf War, the United States used what Secretary of State James Baker called "calculated ambiguity" to dissuade the Iraqis from using their WMD arsenal against coalition forces. This perspective reflected President George Bush's private decision not to respond with nuclear weapons even if the Iraqis used chemical weapons against U.S. forces—but to threaten publicly that he would. U.S. officials believed that this strategy worked and used it again during the winter 1998 confrontation over UN inspections of Iraq's WMD capability.

> *The NASTIs will pose a narrowly focused nuclear threat, characterized by small, fission-type arsenals. . . . [T]he most likely uses for these weapons would be regional attacks to shape crises.*

State Department spokesman James Rubin declared, "We do not rule out in advance any capability available to us."[20] In March 1998, Secretary of Defense William S. Cohen was even more specific, proclaiming, "We've made it very clear to Iraq and to the rest of the world that if you should ever even contemplate using weapons of mass destruction—chemical, biological, any other type—against our forces, we will deliver a response that's overwhelming and devastating."[21]

The problem with making such threats is the ruin that would overtake U.S. deterrent posture if an adversary called the bluff and the administration was forced to recognize the mismatch between its capability, its policy, and its deterrent proclamations. A strong, credible, and more realistic declaratory stance might be: "Use of weapons of mass destruction against the United States, its infrastructure, forces, or allies will result in unrestrained responses at places and with methods of our choosing."

In any deterrence force employment posture, the idea of punishment is central. In the view of Thomas C. Schelling, deterrence can rely on the recognition that "military force can be used to hurt. . . . The power to hurt is bargaining power."[22] The only rational purpose for such pain is to influence enemy decisions, to compel certain actions. Causing pain tends to make the opponent act to avoid it; in international relations, pain or force is threatened in order to make an adversary comply. The deterrer needs to know what the enemy values, while the adversary needs to know what action would trigger or forestall force.[23]

Punishment is versatile. It can be used both for deterrence and for compellence—the difference is timing. While deterrence threatens punishment if the enemy acts in an undesired manner, compellence threatens punishment until the enemy acts in a desired manner. Both cases represent a bargaining process in which the medium of exchange is pain and endurance. Nuclear weapons change the nature of deterrence by enhancing the ability to punish to a point at which, as Schelling observes, "victory is no longer a prerequisite for hurting the enemy." Particularly when mated to ballistic missiles, nuclear weapons can reach the enemy homeland and inflict punishment even if the enemy's armies in the field are intact. This capability also increases the speed of conflict, which enhances their punishment impact but also increases pressure on one's own decision makers.[24]

Even a pragmatic declaratory posture, then, can succeed only if it is supported in practice by an employment policy that provides realistic options for responding to WMD attacks. Information warfare can provide such options. IW techniques act rapidly and can inflict punishment on an enemy homeland; accordingly, they may be useful for certain deterrence applications. Information warfare, as one of the "means of our choosing" in our proposed deterrence posture, can maintain escalation dominance. That is, it can widen the war in ways the enemy cannot match, inflicting damage that is unacceptable to him but not to the international community (as would be the case with nuclear retaliation). A conventional response may be insufficiently persuasive; IW's ability to act directly against vital elements may make it more effective.[25] In the view of authors John Arquilla and David Ronfeldt, "An information offensive aimed at an enemy might seek to deter and dissuade a belligerent society without having to destroy its armed forces. In this, strategic information warfare would resemble prior systems, from strategic bombing to counter-value nuclear targeting."[26]

Information warfare may be even more amenable than nuclear weapons to implementing Schelling's bargaining-and-punishment approach to deterrence, given its specific focus on perception and communication. Schelling's ideas acquired an unfortunate association with the ROLLING THUNDER bombing campaign during the Vietnam War.[27] Perhaps information technology permits their resurrection.

The weapons that could bring back Schelling's bargaining concepts are mainly the tools of the hacker and the "old crows" of the U.S. military electronic warfare community, supplemented by emerging technologies. The techniques most closely associated with information warfare are those of computer network attack. These include viruses and knowledge-robot bombs that target specific computer components. They can be placed in computers in advance as "Trojan horses" (which look like legitimate programs but are actually destructive) or as "trap doors," which provide unauthorized outside access and exploitation. A third approach, "chipping," plants malicious hardware in enemy systems.[28]

In addition, the tools of electronic warfare, used since World War II against enemy sensors, can today, particularly when augmented by advanced technology, be turned against communications and computers. Enemy communications signals and computer functions can be jammed, interfered with, or spoofed. Electromagnetic pulse (EMP) attacks can burn out critical enemy equipment. The brute-force method of generating EMP is to detonate high in the atmosphere a nuclear device optimized to deliver most of its energy as electromagnetic pulse; however, the collateral effects may not be acceptable, and the standing general objections to using nuclear weapons apply. A device known as a high-energy radiofrequency gun, proposed by Winn Schwartau, would achieve the same effect, with the added benefit that it could target specific facilities or even individual computers. At the most exotic extreme, genetically engineered microbes that destroy computers might be developed. These would function in the same way as the bacteria bred to clean up petroleum spills.[29]

At first glance, it is these very capabilities that would seem to pose the greatest threat to the United States itself, dependent as it is on an extensive information infrastructure for governance, finance, civil infrastructure, and military effectiveness. Arguably the United States has the most extensive system of computer networks in the world; it offers plenty of targets to strike. However, that size is also a strength. A network's power increases with its size, and larger size equates to increased survivability, through redundancy.[30]

Conversely, such weaknesses should be all the greater in adversary systems. An entity capable of striking the American information infrastructure must have nodes of its own exposed to attack. In the year 2000, there are estimated to be 262 million Internet users worldwide.[31] This number is estimated to grow to one billion by 2005.[32]

The areas of largest growth in Internet hosts are in the third world; Iran underwent the second-largest increase in the third quarter of

1994, with more than 100 percent growth in three months. Thirty-five percent of Internet hosts are now outside of the United States.[33] If the large United States computer network presents vulnerabilities, how much more susceptible are the smaller networks of adversaries, particularly given the authoritarian penchant for centralized control of communications?[34] These centralized, localized systems would be even easier to enter, and would probably fail much less gracefully, than Western ones.

In a remarkable role reversal for countries that formerly hoped to hang the West by ropes the capitalists sold to them, many third-world countries are attempting to overcome their backwardness, and especially the isolation of their individual communities, by jumping from agricultural economies directly into the modern communications era. These countries buy their communications technologies from the advanced states of the West. By selling them this hardware the United States provides the wherewithal for future conflicts.[35] This is the case especially for developing nations obtaining space infrastructures from multinational consortia; these states substitute satellites, such as Iridium and Globalstar (which the United States also builds), for landlines. On the other hand, by taking this approach, these nations provide doors into their own communications networks.

Given such capabilities and vulnerabilities, the operational question becomes one of what to attack (for coercion) or threaten to attack (for deterrence). Colonel John Warden, the intellectual influence behind the coalition air campaign against Iraq during the Persian Gulf War, proposes a useful framework that conceives of the enemy nation as an interconnected system. His model posits five nested rings, or "centers of gravity." The outside ring represents the military forces that protect the society; in his view, this is the hardest ring to attack, because it is designed to defend itself, and a large number of targets must be destroyed to achieve any meaningful effect. The next ring is the population; this ring was the target of the World War II bombing campaigns and of the countervalue targeting schemes of the early nuclear age, but it comprises the most targets and is a very difficult ring to break. Critical industry resides in the third ring: attacking it strikes at both the enemy's war-making potential and social functioning. The fourth ring contains the "organic essentials," the infrastructure, such as power and transportation, upon which a nation runs. Attacking this ring can have a strong effect on all the others.[36]

The fifth and innermost center-of-gravity ring is national leadership. This ring decides when to fight and when to surrender. It represents the smallest but most vital target set. In Warden's view, this is the ring to focus on in a strategic campaign. It is particularly vulnerable in authoritarian regimes, where the existence of small leadership elites—typically having ill-defined succession processes and not representing the will of the masses—presents an opportunity for changing the nation's entire direction.[37]

To gauge the probable domestic response, consider the reactions during the Persian Gulf War to the Al Firdos bunker bombing or the "highway of death"—and multiply it. The American public abhors both nuclear weapons and high casualties, even among enemies.

IW techniques are especially well suited to attacking targets critical to decision making, as John Arquilla and David Ronfeldt propose. Cyberwar techniques can produce "decapitation" effects. The leaders themselves need not be killed. A vulnerability of authoritarian regimes is that their leaderships must control their societies tightly if they are to stay in power; it is necessary only to destroy their means of doing so—command and control links, internal surveillance and police systems, propaganda networks.[38]

A developing nation trying to compete economically with the modern world can be expected to value highly its infrastructure and industry—such elements as electrical power distribution, telephones, transportation grids, air traffic control, and irrigation. They are likely to be controlled by computer networks that are vulnerable to attack, as Daniel Kuehl suggests. Likewise, some nations have industries or resources that constitute their sole economic lifelines, and these could provide opportunities. For example, an oil-producing nation might suffer particularly if the computer controls for an oil refinery were altered to throw chemical processes out of balance; explosions could result. The computer controls for nuclear reactors that produce weapons-grade fuel might be disrupted. IW can even strike at the morale of civilian populations—through disruption of essential services, but also by the destruction of influential media and even by bogus television broadcasts that "morph" their leaders in compromising ways.[39]

As for counterforce campaigns, information warfare can not only hold military targets at risk, for deterrence purposes, but offer damage-limitation options. Attacking command, control, communications, computers, intelligence, surveillance, or reconnaissance assets would take out a military's brain and nervous system and with it the opponent's ability to orchestrate the employment of forces.[40]

Finally, and crucially, IW can defend against an opponent having WMD and missile technology. Ballistic missiles are space systems, and all such systems have three components: that in space (the missile), that on the ground (the launch station), and the link segment (the communications between the missile and its control station). Antiballistic missiles strike only at the space segment; IW targets all three. It might be possible to jam or inhibit the transmission of the launch order from national authorities. Launch systems might be commanded falsely to send a missile off course. As U.S. opponents try to exploit the Global Positioning System, it might be appropriate to modify the signal to confuse enemy guidance systems. Of course, there is also the brute-force method of "frying" the missile's or launcher's electronics with EMP.

The versatility of information warfare is clear. Because of their discriminating nature, IW techniques can respond to acts either of nonstate actors or their state sponsors. Information warfare—which may not even constitute "force" in the classical or legal sense—provides options to counter proliferation efforts early in the development process. It might even be appropriate to use IW to preempt a conflict.[41]

Costs and Caveats

What would be required to implement a strategy incorporating IW-based deterrence? The move to information warfare in its total scope would be a revolution in military affairs; to integrate even this aspect of such an RMA, doctrinal and organizational adaptations would be required, in addition to technological advances and new systems.[42]

The Department of Defense would need to adjust extensively its structure and policies to accommodate information warfare. One recommendation proposes "standing up" an Information Corps co-equal with the other four armed services. Martin C. Libicki suggests that a separate Information Corps would guide systems acquisition, promote doctrine development, provide unity of command for functions currently spread among separate services, and create an environment for the development of "information warriors."[43] Another approach grants Dr. Libicki's concerns but recognizes that budget constraints will not permit a separate service and instead proposes a functionally oriented unified command to champion the IW mission.[44] At a minimum, it may make sense to collect the IW function under a single already existing unified command.

Information warfare . . . can maintain escalation dominance. That is, it can widen the war in ways the enemy cannot match, inflicting damage that is unacceptable to him but not to the international community.

The military would also have to undertake the costs of developing specialized and technical expertise, upon which information warfare places a high premium. The services would have to invest in scholarships for software engineers, computer architects, and electrical engineers in order to grow an initial knowledge base. Because computer intrusion is not a skill taught in universities, it would be necessary to supplement academic programs with training by industry or Defense Department agencies. Such personnel would need to be carefully screened and monitored—perhaps in a system similar to the Defense Department's Personnel Reliability Program, currently applied to service people with responsibilities involving nuclear weapons—to ensure that these skills remain under strict control and discipline. Congress might also choose to exercise the kind of oversight and approval over IW activities that it currently does for covert intelligence activity, so as to mute any public concern over government-sanctioned and funded hackers.

The military would be competing with an expanding knowledge-industries economy, so it would be necessary to consider retention incentives. Those who joined the military to enter the IW field would need assurance of reasonable career prospects; the services may need to reexamine their promotion criteria to ensure that they are not unduly biased in favor of "movers and shooters." Overcoming the military's traditional "machismo" image of leadership enough to allow a vital community to emphasize "brains over brawn" and create "cyber warriors" might be the hardest adaptation of all.[45]

Skilled people are essential to answering the critical doctrinal questions that underlie successful IW campaigns. Orchestration would be necessary to avoid fratricide or undesired interactions. For instance, it may not make sense to strike enemy communications systems with conventional weapons while operations to penetrate and take out computer capabilities are pending. More importantly, the level of command or government having release authority for IW attacks must be clarified. Perhaps the president would need a second "football" for information-warfare options.

The focus of the services' systems procurement efforts would need to shift. In the IW paradigm, the network is more important than any specific platform. In an IW campaign, these systems assume more significance than they have in their force-enhancement role; they become gunsights and weapons.[46] National agencies would need to develop intelligence capabilities that permit them to understand enemy information networks and their specific weaknesses. Spending would have to increase for research and development of some exotic systems, such as high-energy radiofrequency guns. The Defense Department would also have to ante up to protect its information systems and the national infrastructure.

It may also be appropriate to reconsider policies regarding export controls and technology transfer. After all, if the United States sells the hardware, it retains the advantage of understanding its operation and capabilities and can potentially control design and manufacturing to the benefit of the IW program. Technology export policy must balance the opportunity for exploitation against the risk that the technology might be used against U.S. interests.

An information-warfare strategy option for deterrence and coercion carries other risks that require consideration. IW is not a cure-all. Not all opponents will have information systems that are vulnerable and that matter to them; a politically reclusive nation with an information architecture closed to the outside world would be difficult to attack. (Of course, such a closed system would have forfeited the interconnectivity that is the strength of cyberspace.) Further, the use of IW for deterrence or coercion may invite retaliation in kind. As in the nuclear era, political decision makers must consider carefully how close to the brink to go.

The nonlethal nature of an IW response may make it less than compelling to some opponents. However, not even nuclear responses are guaranteed to deter all adversaries. The civilian leaders of a WMD power may have poor control over its military at a time when its behavior heightens the risk of nuclear confrontation. Regional militaries may be biased in favor of offensive postures and preventive war.[47] Deterrence could fail because an enemy leader misreads the depth of U.S. political support in a crisis. Cultural factors may color his calculations. A tyrant surrounded by sycophants, the center of a personality cult, may not learn of his danger until it is too late; even then, such a leader may be indifferent toward the degradation of his own society or economy. Individual leaders or whole populations—the NASTI states are likely to be among these—may have worldviews or value sets that simply make them undeterrable. Others may perceive their situations as so dire as to leave them nothing to lose; they might be inclined to launch revenge attacks, to go out in a blaze of glory. Finally, of course, accidental or unauthorized launching of WMD from a state experiencing civil unrest cannot be deterred, whether by IW, nuclear, or conventional response.[48] Because IW will not be universally applicable, American decision makers will need to retain other options. For the exceptionally hard to deter threats, a nuclear response might be the only alternative. Conventional attacks using precision guided weapons may suffice in some instances, but such responses require prolonged military campaigns and thus extended commitments of people and resources.

The vital interests of protecting security, building the economy, and promoting democratic values will continue to lead the United States to participate in coalitions, support friends, and confront adversaries. Some of those adversaries will possess nuclear, biological, or chemical weapons. Others will add ballistic missiles to their arsenals. More will strive to join the NASTI club to exploit the leverage these weapons offer for shaping crises to their advantages. The United States needs the capability to deter the use of WMD, devalue their ownership, and coerce their owners.

Information warfare offers U.S. decision makers ways to accomplish these ends with a versatility and credibility that nuclear weapons lack. Computer network attack, electronic warfare, and electromagnetic pulse devices represent a range of options for threatening punishment against the targets adversaries may well value, and they can help to limit the ability of an enemy to strike at U.S. forces or allies.

Information warfare would require extensive adaptation, investment in personnel and technology, and revision of organization and doctrine. Perhaps most importantly, policy makers will need to recognize that IW is not a panacea. It offers much, and can probably fulfill much. Yet IW may not fit every crisis. As always, government and military leaders will need to balance opportunity and risk.

Notes

1. For an overview of the various terms, see Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: National Defense Univ., 1995).

2. Arthur K. Cebrowski [Vice Adm., USN] and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," U.S. Naval Institute *Proceedings*, January 1998, pp. 28–35.

3. Joint Staff, *Command and Control Warfare*, CJCS MOP 30 (Washington, D.C.: Joint Staff, 8 March 1993), encl. 1, pp. 1–32.

4. Philip L. Ritcheson, "Proliferation and the Challenge to Deterrence," *Strategic Review*, Spring 1995, p. 39.

5. Central Intelligence Agency, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January through 30 June 1999*, retrieved 11 March 2000 from the World Wide Web: http://www.cia.gov/cia/publications/bian/bian_fer_2000.htm/#scopenote.

6. George J. Tenet, "Statement by Director of Central Intelligence," in Senate Select Committee on Intelligence, *The Worldwide Threat in 2000: Global Realities of Our National Security*, 2 February 2000, retrieved 11 March 2000 from the World Wide Web: http://www.cia.gov/cia/public_affairs/speeches/dci_speech_020200.html.

7. Robert D. Walpole, "Statement for the Record," in Senate Subcommittee on International Security, Proliferation, and Federal Services, *The Ballistic Missile Threat to the United States*, 9 February 2000, retrieved 11 March 2000 from the World Wide Web: http://www.cia.gov/cia/public_affairs/speeches/info_speech_020900.html.

8. Barry R. Schneider, "Strategies for Coping with Enemy Weapons of Mass Destruction," *Airpower Journal*, Special Edition 1996, pp. 36–47, retrieved 2 April 1998 from the World Wide Web: www.cdsar.af.mil/apj/schneider.html.

9. Central Intelligence Agency, *Unclassified Report to Congress*.

10. Robert G. Joseph, "Regional Implications of NBC Proliferation," *Joint Force Quarterly*, Autumn 1995, pp. 65–7, retrieved 8 April 1998 from the World Wide Web: www.dtic.mil/doctrine/Jel/JFQ-pubs/1709.pdf.

11. Central Intelligence Agency, *Unclassified Report to Congress*.

12. Ibid.

13. Ibid.

14. Dean Wilkening and Kenneth Watman, *Nuclear Deterrence in a Regional Context* (Santa Monica, Calif.: RAND, 1995), pp. 23–7.

15. Ritcheson.

16. Joseph, pp. 68–9; Schneider, pp. 1–3, 36–47; Wilkening and Watman, pp. 32–8; and Ritcheson, p. 40.

17. John Arquilla and David Ronfeldt, "Cyberwar Is Coming," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), pp. 47–8; and Schneider, pp. 36–47.

18. Ritcheson, pp. 41–3.

19. Wilkening and Watman, pp. 10–3, 21.

20. Stephen I. Schwartz, "Miscalculated Ambiguity: U.S. Policy on the Use and Threat of Use of Nuclear Weapons," *Disarmament Diplomacy*, February 1998, pp. 1–3, retrieved 26 March 1998 from the World Wide Web: www.brook.edu/fp/projects/nucwost/threats.htm.

21. William S. Cohen, "WMD Poses Top-Priority Threat to America," *Defense Issues*, 17 March 1998, retrieved 8 May 1998 from the World Wide Web: www.defenselink.mil/pubs/di98/di1316.html.

22. Thomas C. Schelling, *Arms and Influence* (New Haven, Conn.: Yale Univ. Press, 1966), p. 2.

23. Ibid., pp. 3–4.

24. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard Univ. Press, 1980), pp. 195–201; and Schelling, *Arms*, pp. 7, 18–26, 33–4.

25. Wilkening and Watman, pp. 40–2; and Schneider, pp. 36–47.

26. John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp—Section 1," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, Calif.: RAND, 1997), p. 159.

27. For insight into the role of Schelling's ideas in Vietnam, see Mark Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam* (New York: Free Press, 1989). See also Earl H. Tilford, Jr., *Setup: What the Air Force Did in Vietnam and Why* (Maxwell Air Force Base, Ala.: Air Univ. Press, 1991).

28. Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force," *Naval War College Review*, Spring 1998, pp. 8–13; John L. Petersen, "Info War: The Next Generation," U.S. Naval Institute *Proceedings*, January 1997, pp. 60–2; and David L. Potter, "Information Warfare: Malicious Software and Technology," *Military Intelligence*, January–March 1997, pp. 34–7. For the best discussion of information warfare tools and techniques, see Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), pp. 95–136, 160–70.

29. Keith D. Anthony, "Information Warfare: Good News and Bad News," *Military Intelligence*, January–March 1997, pp. 31–3; Scot W. Merkle, "Non-Nuclear EMP: Automating the Military May Prove a Real Threat," *Military Intelligence*, January–March 1997, pp. 37–9; Petersen, p. 62; and Schwartau, pp. 171–89.

30. Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (Washington, D.C.: National Defense Univ. Press, 1994), pp. 11–5.

31. "Global Internet Statistics (by Language)," retrieved 25 March 2000 from the World Wide Web: http://www.euromktg.com/globstats/index.html.

32. Robert O. Keohane and Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," *Foreign Affairs*, September/October 1998, p. 82.

33. Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1995), p. 182.

34. A prime example is how the Internet has evolved in Cuba. See Patrick Symees, "Che Is Dead," *Wired*, February 1998, pp. 140–6, 178–9, 188–9.

35. Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, Va.: AFCEA International Press, 1996), pp. 231–42.

36. John A. Warden III [Col., USAF], "The Enemy as a System," *Airpower Journal*, Spring 1995, pp. 41–55.

37. Ibid.

38. Daniel T. Kuehl, "Strategic Information Warfare and Comprehensive Situational Awareness," in Campen, Dearth, and Goodden, eds., pp. 185–95; and Arquilla and Ronfeldt, "Cyberwar," pp. 47–8.

39. Kuehl, p. 192. See also Szafranski; and Campen, Dearth, and Goodden, eds., pp. 236–40.

40. Arquilla and Ronfeldt, "Information, Power, and Grand Strategy," p. 157.

41. Barnett, pp. 14–7; and Arquilla and Ronfeldt, "Cyberwar," pp. 48–54.

42. James R. FitzSimonds and Jan M. Van Tol, "Revolutions in Military Affairs," *Joint Force Quarterly*, Spring 1994, pp. 24–31; Andrew F. Krepinevich, "From Cavalry to Computer: The Pattern of Military Revolutions," in *Strategy and Force Planning*, ed. Strategy and Force Planning Faculty, 2d ed. (Newport, R.I.: Naval War College Press, 1997), pp. 430–46.

43. Libicki, *The Mesh and the Net*, pp. 52–69; and Martin C. Libicki and James A. Hazlett, "Do We Need an Information Corps?" *Joint Force Quarterly*, Autumn 1993, pp. 88–97.

44. See the author's "An Information Corps: Has Its Time Come Yet?" (manuscript, Naval War College, Newport, R.I., 20 October 1997).

45. Libicki, "Information Corps," pp. 88–97; Douglas H. Dearth, "Information War: Rethinking the Application of Power in the 21st Century," *Military Intelligence*, January–March 1997, pp. 13–6.

46. Cebrowski and Garstka, pp. 28–35.

47. Scott D. Sagan, "The Perils of Proliferation: Organization Theory, Deterrence Theory, and the Spread of Nuclear Weapons," *International Security*, Spring 1994, pp. 66–107.

48. Ritcheson, pp. 41–3; and Schneider, pp. 36–47.

Ψ